FONDAZIONE EDMUND MACH

ISTITUTO AGRARIO
DI SAN MICHELE ALL'ADIGE

DIREZIONE SISTEMI INFORMATIVI
Ufficio servizi Informatici

Prot. n. 0009001/MC/MR San Michele a/A, 20 DIC. 2011

Documento descrittivo del processo di accreditamento degli utenti dell'Organizzazione Fondazione Edmund Mach

Rel. 2.2 20/12/2011

Il presente documento denominato DOPAU, è sottoscritto dal dirigente dei sistemi Informativi della Fondazione Edmund Mach, Dott. Ing. Massimo Carnevali

Il dirigente dei sistemi informativi
- *Ing. Massimo Carnevali* -

Dirigente
Sistemi Informativi,
Organizzazione e Comunicazione
- *Ing. Massimo Carnevali* -

Nota introduttiva

La partecipazione alla Federazione IDEM ("Federazione") abilita l'organizzazione partecipante ("Partecipante") ad utilizzare la tecnologia di Shibboleth di condivisione degli attributi relativi alle identità per gestire l'accesso alle risorse on-line che possono essere rese disponibili all'interno della comunità IDEM. Un obiettivo della Federazione è quello di sviluppare, nel tempo, degli standard per le organizzazioni al fine di assicurare che le asserzioni sugli attributi che vengono scambiate siano sufficientemente robuste e fidate per gestire l'accesso ad importanti risorse protette. Con la crescita della fiducia interna, la Federazione spera che i Partecipanti alla fine possano fidarsi dei sistemi di identity management e dei sistemi di gestione di accesso alle risorse degli altri partecipanti come si fidano dei propri.

Fondamentalmente ci si aspetta dai Partecipanti che essi forniscano agli altri Partecipanti asserzioni sugli attributi autorevoli e accurate e che ciascuno riceva asserzioni sugli attributi protette e nel rispetto dei vincoli di privacy imposti dalla Federazione o dalla fonte delle informazioni. Per raggiungere tale obiettivo IDEM richiede che ogni Partecipante renda disponibile agli altri Partecipanti certe informazioni di base riguardanti il proprio sistema di identity management, incluse le informazioni relative agli attributi che vengono utilizzati per la Federazione.

I due criteri per garantire che gli Identity Provider forniscano asserzioni di attributi fidate sono: (1) che il sistema di gestione delle identità ricada sotto la supervisione degli organismi che hanno responsabilità direttive e gestionali nell'Organizzazione e che (2) il sistema che emette le credenziali per gli utenti finali (e.g., PKI certificates, userids/passwords, Kerberos principals, etc.) sia dotato di appropriate misure di gestione del rischio (e.g., authentication and authorization standards, security practices, risk assessment, change management controls, audit trails, etc.)

Il Documento DOPAU prodotto dal Partecipante DEVE contenere le informazioni elencate nel presente modello.

In caso di modifica delle procedure o informazioni descritte nel documento, esso DEVE essere prontamente aggiornato e ne deve essere data comunicazione alla Federazione.

Abbreviazioni

Abbrevizione	**Descrizione**
FEM	Fondazione Edmud Mach
DSI	Direzione dei sistemi informativi
S1P S2P	Sistemi gestione economico giuridica del personale
CIF	Centro istruzione e formazione della Fondazione
CRI	Centro ricerca ed innovazione della Fondazione
CTT	Centro trasferimento tecnologico della Fondazione
SAM	Servizio Amministrativo della Fondazione

Gestore dell'accreditamento

La gestione delle identità digitali è in carico alla Direzione dei Sistemi Informativi della Fondazione (DSI). La DSI gestisce tutte le informazioni relative all'identità digitale di accesso alla rete ed ai suoi servizi, coordina i processi di accreditamento ed il rilascio delle credenziali.
Tutte le identità sono gestite dall'unico sistema di account basato su LDAP Active Direcory- Microsoft le cui prerogative sono:

- unica identità digitale per ogni individuo e relativo accesso ai servizi del network
- univocità di associazione delle credenziali rilasciate con l'identità dell'individuo.
- Traccia e gestione automatica delle credenziali in relazione alla durata del rapporto della persona in Fondazione
- Caratterizza gli account associando le opportune policy per l'accesso a specifiche risorse e servizi messi a disposizione dal network.

Il responsabile della base dati è il dirigente della DSI.

Utenti gestiti e mappature affiliazione IDEM:
La tabella n1. riassume i ruoli gestiti e le affiliazioni IDEM associate. E' da rilevare che nonostante siano presenti e gestiti categorie e profili di utenza diversi, solo ad alcuni di essi è concesso l'utilizzo dei servizi NILDE con relativa popolazione del campo di affiliazione IDEM associato.

Descrizione ruolo	Significato ruolo	Affiliazione IDEM
Ricercatore		staff
Personale Docente		staff
Collaboratore didattico	assistenti	staff
Tesista	Personale assegnato comparto ricerca	staff
Borsista	Personale assegnato comparto ricerca	staff
Collaboratore alla ricerca		staff
Studente		Student
Personale tecnico a tempo det/indet	Personale assegnato al comparto trasferimento Tecnologico	staff
Personale amministrativo		staff

Visione d'insieme del processo di accreditamento degli utenti:
Il processo di accreditamento per l'utenza è sinteticamente rappresentato nelle figura n.2 e propone una visione d'insieme di processi organizzativi, procedure automatizzate e flussi logici che portano alla gestione delle credenziali dell'utente. Le principali risorse e tecnologie coinvolte nel processo sono i sistemi di gestione economico-giuridica del personale (S1P-S2P) le cui informazioni sono presentate ai sistemi di directory ed autenticazione della Fondazione basati su Active Directory.
L'architettura è rappresentata sinteticamente dal diagramma in Fig. 1:

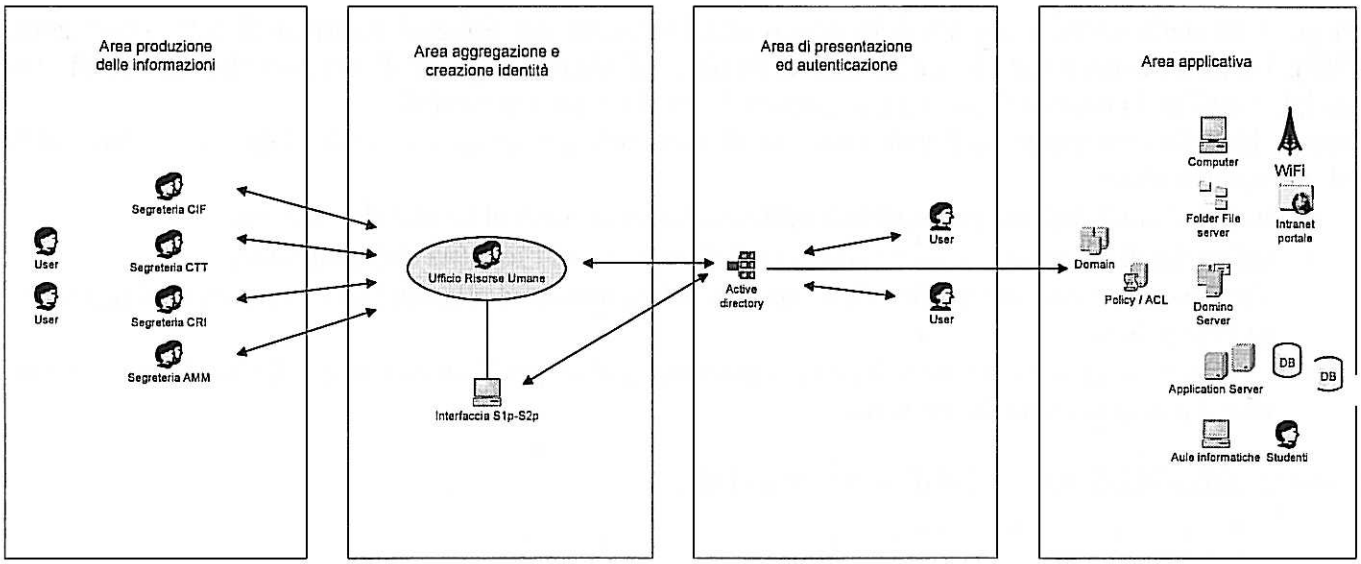

Fig. 1 Visione d'insieme del processo di accreditamento sintetico degli utenti

Nello schema sono evidenziate e coinvolte 4 aree principali oltre all'utenza richiedente:

- **Area di produzione delle informazioni**: le segreterie dei centri di area (CIF, CRI, CTT, SAM) raccolgono le informazioni necessarie al processo di sottoscrizione del contratto o collaborazione con la Fondazione.
- **Area di aggregazione delle informazioni e creazione dell'identità digitale**: l'ufficio risorse umane provvede all'aggregazione dei dati, alla formalizzazione del rapporto contrattuale ed alla creazione dell'identità digitale cui è associato un profilo anagrafico, economico giuridico.
- **Area di presentazione ed autenticazione:** è la sintesi ultima del processo che associa all'identità digitale, i profili e le ACL corrispondenti ai servizi ICT cui l'utente deve essere abilitato alla fruizione (Active directory - ufficio servizi informatici).
- **Area applicativa:** alcuni esempi di servizi e risorse che l'utenza può utilizzare in funzione del proprio profilo associato all'identità digitale.

Processo di accreditamento per le categorie di utenti gestite

Il diagramma in Fig. 2 "Processo di accreditamento sintetico", descrive le principali fasi e gli attori coinvolti nel processo di rilascio e di revoca (o blocco) delle credenziali di accesso al network della Fondazione ed ai suoi servizi.

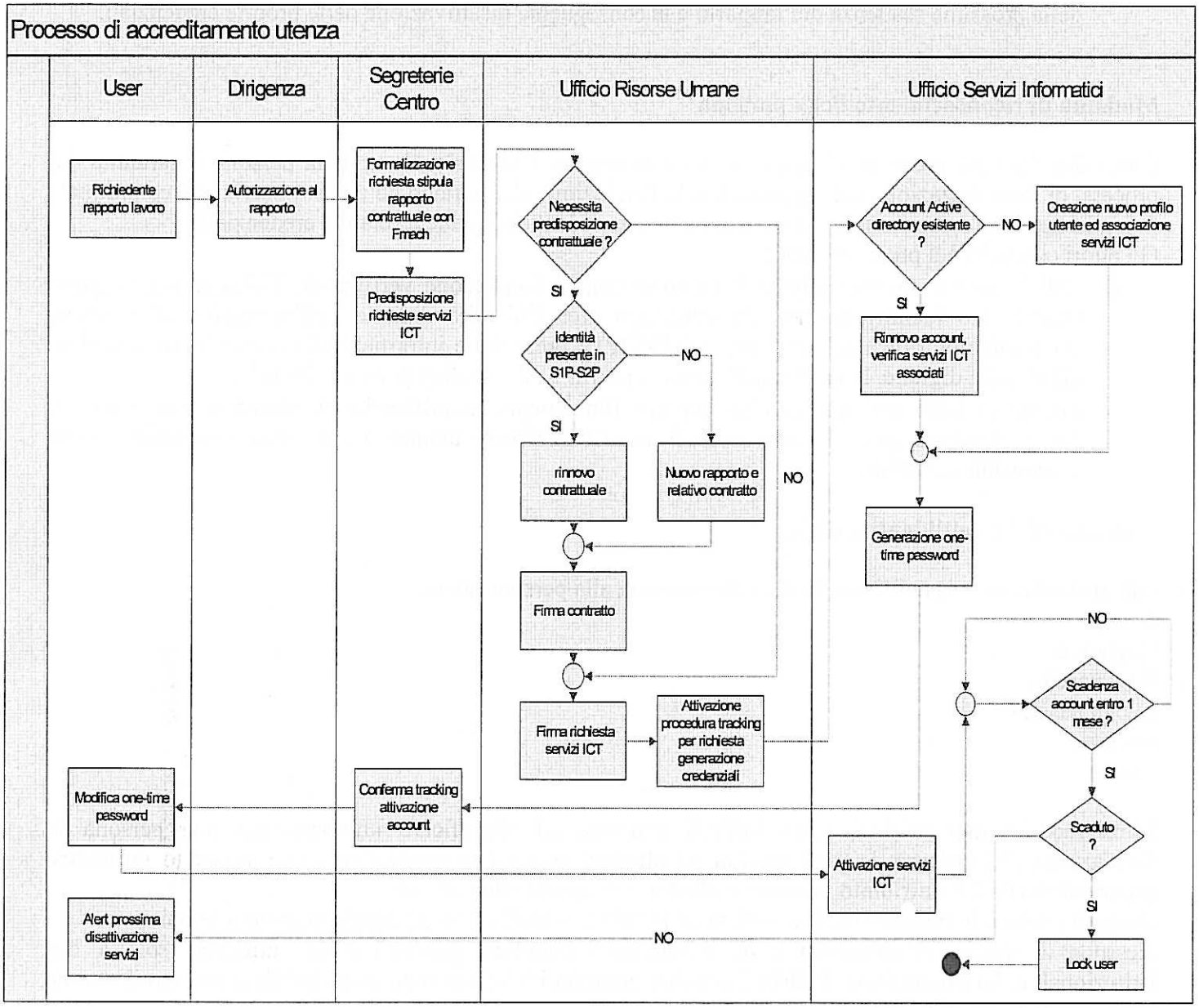

Fig. 2 Processo di accreditamento sintetico

Gli aspetti fondamentali del processo si possono riassumere nelle seguenti attività:

1. **Autorizzazione:**
   - esplicita da parte della dirigenza nel formalizzare un rapporto con la fondazione (contratto, collaborazione, consulenza)
   - implicita a seguito dell'iscrizione ad uno specifico percorso formativo (secondaria superiore, professionale, universitario).
2. **Verifica della presenza dell'identità/account nei sistemi S1P-S2P/Active directory:** Step importante per garantire l'univocità delle credenziali associate all'utenza, cui segue un rinnovo delle credenziale con verifica dei ruoli associati o creazione di nuova identità.
3. **Rilascio delle credenziali:** tramite un processo di ticket tracking che traccia tutto l'iter di rilascio attraverso le segreterie dei centri che hanno seguito l'iter di formalizzazione del rapporto per l'utente richiedente e che sono in possesso di tutta la necessaria anagrafica per l'identificazione.

4. **Locking credenziali:** un processo automatico basato su campi in Active directory popolati con dati forniti in fase di sottoscrizione del rapporto con la fondazione (end date) informa l'utente della prossima scadenza del rapporto e la conseguente disattivazione delle proprie credenziali.

Modalità di riconoscimento della persona

Come descritto nel processo sintetico di accreditamento, l'identificazione della persona è garantita dai processi di formalizzazione del rapporto con la Fondazione che portano ad una sottoscrizione contrattuale (o iscrizione a percorso formativo) cui è associata una identità digitale e relative credenziali.
Gli attori coinvolti nel processo sono:

- Ufficio risorse umane: stipula il rapporto con la Fondazione verificando l'identità del soggetto (documento identificazione). Al contempo crea l'identità digitale nell'anagrafica di gestione economico giuridica del personale (S1P-S2P) e presenta le informazioni necessarie per associare all'identità digitale, le credenziali, dunque profili e ACL/policy per i servizi ICT.
- Segreteria CIF: verifica identità studente (documento identificazione), attraverso procedura di flusso standard, passa le informazioni ad ufficio risorse umane che richiede la creazione della credenziale associata.

Caratteristiche dell'identità digitale:

Gli attributi (minimi) dell'identità digitale associata alla persona sono:
Nome
Cognome
Data nascita
Luogo nascita
Nazione
Sesso

L'insieme dei dati minimi sopra indicati concorre ad identificare univocamente una persona in Fondazione. All'insieme dei dati minimi ed ulteriori presenti in anagrafica viene associato un codice (matricola S1P-S2P) attribuito in modo esclusivo e perpetuo alla persona.
Ad ogni persona in Fondazione è associato un indirizzo e-mail ed un eventuale numero telefonico.
Nessuna di queste informazioni è da considerarsi pubblica, possono essere utilizzate solo a fini istituzionali della Fondazione. Indirizzi e-mail e numeri di telefono sono consultabili attraverso il portale istituzionale (se pubblicati).

Gestione del ciclo di vita:
Una volta formalizzato il rapporto della persona con la fondazione, l'informazione riguardante il ciclo di vita dell'account viene trasferita sui sistemi Active directory che, con procedure automatiche, si occupano delle notifica e successiva disattivazione dell'account coincidente con la conclusione del rapporto con la Fondazione. Le situazioni che modificano il ciclo di vita di un account (cessazione, trasferimenti..) fanno scaturire nuovamente il processo che, dalla fonte uff. risorse umane e relativi sistemi S1P-S2P, presenta il nuovo dato ai sistemi Active directory per l'opportuno aggiornamento.

Formato e regole delle credenziali.
Le credenziali elettroniche che formano l'account in Fondazione sono composte da username e password.
Ogni persona possiede un unico account di accesso al network ed ai servizi messi a disposizione della rete.
L'account è nella forma XYZ, ove:
X=cognome, Y=1° lettera nome, Z=progressivo numerico (in caso omonimia), il tutto nell'ambito di max 10 caratteri.

La password è una stringa alfanumerica di lunghezza minima 10 caratteri, non può essere uguale alla precedente utilizzata, deve obbligatoriamente essere cambiata ogni 3 mesi.

Modalità di consegna delle credenziali:
Al momento della creazione delle credenziali, il processo di tracking informa la segreteria di centro dell'avvenuta attivazione dell'account con relativa one-time password random.
Le segreterie competenti si occupano di comunicare individualmente le credenziali di accesso ai rispettivi richiedenti.
Le persone che hanno ottenute le prime credenziali, debbono obbligatoriamente effettuare un cambio password per poter accedere ai servizi di rete.

Modalità di recupero delle credenziali.
Il recupero di una credenziale smarrita avviene presentandosi presso l'ufficio servizi informatici che adempie alla re-inizializzazione delle credenziali previa verifica dell'identità dell'individuo.
Alla password rigenerata, segue l'iter descritto nel paragrafo precedente.

Modalità di gestione e smarrimento smartcard/token.
Al momento non vengono rilasciate smartcard o token.

Durata dell'accreditamento:
Può essere a tempo determinato, indeterminato, ed è direttamente collegata al tipo ed alla durata del rapporto tra la persona e la Fondazione.

Disabilitazione dell'utente
La disabilitazione dell'account avviene automaticamente sulla base dei parametri di durata del rapporto tra persona e Fondazione.
Alla data di fine rapporto può essere previsto un breve periodo di estensione necessario all'eventuale espletamento delle procedure di uscita dalla Fondazione.

Cancellazione definitiva utente:
Nei sistemi S1P S2P, il codice matricola associato in modo esclusivo alla persona, permane indefinitamente nel DB anche a seguito della scadenza contrattuale. Diversamente, il relativo accout in Active directory rimane bloccato ma presente per 6 mesi successivi alla scadenza contrattuale, in vista di possibile riattivazione per instaurazione di nuovo rapporto. A seguito dei 6 mesi, viene rimosso dalla base dati.

Rischi specifici associati alla categoria utenti
I rischi ed i problemi associati a questa categoria di utenti sono essenzialmente:

1. I tempi di rilascio delle credenziali, subordinati ai tempi amministrativi per la formalizzazione contrattuale.
2. La consapevolezza dei rischi e delle conseguenze inerenti un utilizzo scorretto delle proprie credenziali personali.

Per le problematiche evidenziate nel punto 1, sono state introdotte procedure il più possibile automatiche in modo da minimizzare i tempi di propagazione delle informazioni tra i diversi comparti che concorrono alla creazione delle credenziali.
Per l'ultimo punto, si evidenzia che all'atto della sottoscrizione contrattuale, l'utente riceve copia del "documento di accesso ai servizi di rete" nel quale prende visione e sottoscrive i termini con i quali vengono erogati i servizi di rete.
Oltre a ciò, si sta operando con una costante sensibilizzazione dell'utenza informando ed esponendo concetti di privacy, responsabilità e conseguenze inerenti una scorretta gestione delle credenziali personali.

Interoperabilità tra credenziali deboli (username+pwd) ed eventuali credenziali forti (smartcrad)
Al momento non dono implementate credenziali forti.

Il sistema di autenticazione e autorizzazione interno.
Il sistema di gestione delle identità S1P, S2P è la fonte da cui vengono estratti gli elementi essenziali e necessari a create le credenziali di accesso al network e servizi basato su Active directory.
Dalle credenziali citate ed in base alla conseguente validità temporale, si ha accesso a tutti i dati e servizi cui permette lo specifico profilo utente.

Partecipazione ad altre federazioni:
Al momento non sono previste partecipazioni ad altre federazioni che coinvolgano account e ruoli utente.